A

$x \in_R Z_q$ _(102)_

$X = g^x \bmod P$ _(104)_

B

$Y \in_R Z_q$ _(108)_

$Y = g^Y \bmod P$ _(110)_

$S = X^Y \bmod P$ _(116)_

X _(106)_ →

← Y _(112)_

$S = Y^x \bmod P$ _(114)_

FIG. 1

A   **B**

202: $x \in_R \mathbb{Z}_q$

204: $m = g^x \cdot (H_1(A,B,\pi))^r \mod P$

206: $m \longrightarrow$

208: TEST $m \stackrel{?}{\equiv} 0 \mod P$

210: $y \in_R \mathbb{Z}_q$

212: $\mu = g^y \mod P$

214: $\sigma = \left(\dfrac{m}{(H_1(A,B,\pi))^r}\right)^y \mod P$

216: $k = H_{2a}(A,B,m,\mu,\sigma,\pi)$

218: $\longleftarrow \mu, k$

220: $\sigma = \mu^x \mod P$

222: TEST $k \stackrel{?}{=} H_{2a}(A,B,m,\mu,\sigma,\pi)$

224: $k' = H_{2b}(A,B,m,\mu,\sigma,\pi)$

226: $K = H_3(A,B,m,\mu,\sigma,\pi)$

228: $k' \longrightarrow$

230: TEST $k' \stackrel{?}{=} H_{2b}(A,B,m,\mu,\sigma,\pi)$

232: $K = H_3(A,B,m,\mu,\sigma,\pi)$
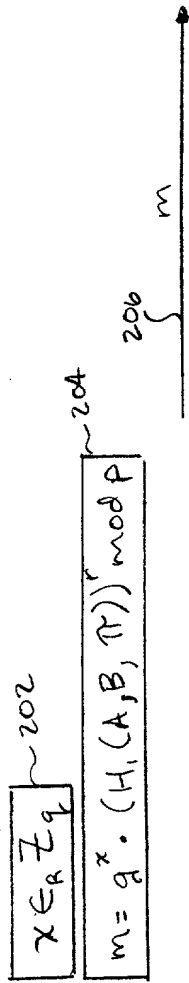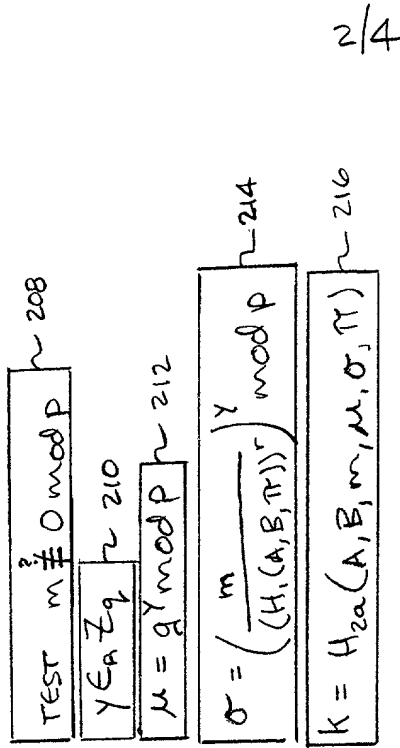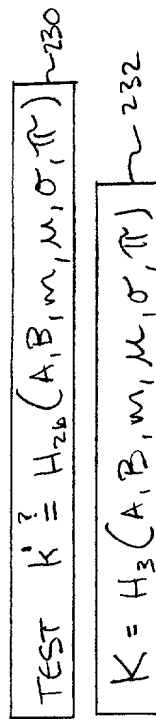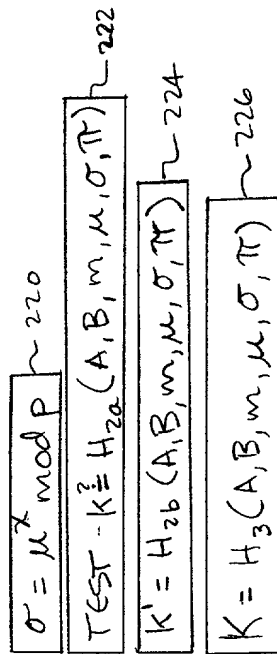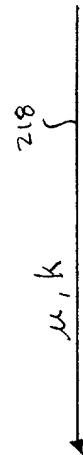
FIG. 2

A

$x \in_R \mathbb{Z}_q$ ~302

$h \in_R \mathbb{Z}_p^*$ ~304

$m = g^x \circ h^q \cdot H_1(A,B,\pi)$ ~306

308 ⟶ m

B

TEST $m \stackrel{?}{\not\equiv} 0 \mod P$ ~310

$y \in_R \mathbb{Z}_q$ ~312

$\mu = g^y \mod P$ ~314

$\sigma = \left(\left(\frac{m}{H_1(A,B,\pi)}\right)^r\right) y^{r^{-1} \mod q}$ ~316

$k = H_{2a}(A,B,m,\mu,\sigma,\pi)$ ~318

320 ⟶ μ, k

$\sigma = \mu^x \mod P$ ~322

TEST $k \stackrel{?}{=} H_{2a}(A,B,m,\mu,\sigma,\pi)$ ~324

$k' = H_{2b}(A,B,m,\mu,\sigma,\pi)$ ~326

$K = H_3(A,B,m,\mu,\sigma,\pi)$ ~328

330 ⟶ k'

TEST $k' \stackrel{?}{=} H_{2b}(A,B,m,\mu,\sigma,\pi)$ ~332

$K = H_3(A,B,m,\mu,\sigma,\pi)$ ~324

FIG. 3

"A" (CLIENT) 402

I/O DEVICES	408-A
PROCESSOR	410-A
MEMORY	412-A

NETWORK 406

"B" (SERVER) 404

I/O DEVICES	408-B
PROCESSOR	410-B
MEMORY	412-B

FIG. 4